小马哥的 Java 项目实战营

Java EE 项目 - 第十一节 应用容器安全

小马哥（mercyblitz）

我是谁?

小马哥（mercyblitz）

- 父亲
- Java 劝退师
- Apache Dubbo PMC
- Spring Cloud Alibaba 架构师
- 《Spring Boot 编程思想》作者

议题

- Web 安全
- 访问控制
- 问答互动

Web 安全

- CSRF

  跨站请求伪造（英语：Cross-site request forgery），也被称为one-click attack或者session riding，通常缩写为CSRF 或者XSRF， 是一种挟制用户在当前已登录的Web应用程序上执行非本意的操作的攻击方法。

- 术语解释
  - CSRF Token

    服务端为客户端生成令牌，该令牌将用于请求合法性校验，一般通过请求头或请求参数传递到服务端

Web 安全

- 术语解释
  - CSRF Token 仓库

  服务端组件，用于从请求加载或生成 CSRF Token。Spring Security 提供了Cookie 和 HttpSession 两种实现。
  - CSRF 请求校验匹配器

  服务端组件，用于判断请求是否需要CSRF校验

Web 安全

- Tomcat CSRF 实现
  - org.apache.catalina.filters.CsrfPreventionFilter
    - 初始化参数

Attribute	Description
denyStatus	HTTP response status code that is used when rejecting denied request. The default value is `403`.
entryPoints	A comma separated list of URLs that will not be tested for the presence of a valid nonce. They are used to provide a way to navigate back to a protected application after having navigated away from it. Entry points will be limited to HTTP GET requests and should not trigger any security sensitive actions.
nonceCacheSize	The number of previously issued nonces that will be cached on a LRU basis to support parallel requests, limited use of the refresh and back in the browser and similar behaviors that may result in the submission of a previous nonce rather than the current one. If not set, the default value of 5 will be used.
randomClass	The name of the class to use to generate nonces. The class must be an instance of `java.util.Random`. If not set, the default value of `java.security.SecureRandom` will be used.

Web 安全

- XSS

  跨站脚本（英语：Cross-site scripting，通常简称为：XSS）是一种网站应用程序的安全 漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就 会受到影响。这类攻击通常包含了HTML以及用户端脚本语言。

  XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页， 使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript， 但实际上也可以包括Java，VBScript，ActiveX，Flash或者甚至是普通的HTML。攻击成功后， 攻击者可能得到更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。

Web 安全

- Tomcat HTTP 头安全实现
  - org.apache.catalina.filters.HttpHeaderSecurityFilter

Attribute	Description
hstsEnabled	Will an HTTP Strict Transport Security (HSTS) header (`Strict-Transport-Security`) be set on the response for secure requests. Any HSTS header already present will be replaced. See RFC 6797 for further details of HSTS. If not specified, the default value of `true` will be used.
hstsMaxAgeSeconds	The max age value that should be used in the HSTS header. Negative values will be treated as zero. If not specified, the default value of `0` will be used.
hstsIncludeSubDomains	Should the includeSubDomains parameter be included in the HSTS header. If not specified, the default value of `false` will be used.
hstsPreload	Should the preload parameter be included in the HSTS header. If not specified, the default value of `false` will be used. See https://hstspreload.org for important information about this parameter.
antiClickJackingEnabled	Should the anti click-jacking header (`X-Frame-Options`) be set on the response. Any anti click-jacking header already present will be replaced. If not specified, the default value of `true` will be used.
antiClickJackingOption	What value should be used for the anticlick-jacking header? Must be one of `DENY`, `SAMEORIGIN`, `ALLOW-FROM` (case-insensitive). If not specified, the default value of `DENY` will be used.
antiClickJackingUri	If ALLOW-FROM is used for **antiClickJackingOption**, what URI should be allowed? If not specified, the default value of an empty string will be used.
blockContentTypeSniffingEnabled	Should the header that blocks content type sniffing (`X-Content-Type-Options`) be set on every response. If already present, the header will be replaced. If not specified, the default value of `true` will be used.
xssProtectionEnabled	Should the header that enables the browser's cross-site scripting filter protection (`X-XSS-Protection: 1; mode=block`) be set on every response. If already present, the header will be replaced. If not specified, the default value of `true` will be used.

THANKS!